ЛЕКЦИОННЫЕ МАТЕРИАЛЫ

Б2.В,ДВ.3.1 «Математические основы криптологии 11504»

(наименование дисциплины (модуля) в соответствии с учебным планом)

Уровень	бакалавриат, специалитет
	(бакалавриат, магистратура, специалитет)
Форма обучения	очная
	(очная, очно-заочная, заочная)
Направление(-я) подготовки	10.05.02 «Информационная безопасность»
	(код(-ы) и наименование(-я))
Институт	комплексной безопасности и специального приборостроения (ИКБ и СП)
	(полное и краткое наименование)
Кафедра	Защита информации (КБ-1)
	(полное и краткое наименование кафедры, реализующей дисциплину (модуль))
Лектор	Доцент Дедов Олег Петрович
	(сокращенно – ученая степень, ученое звание; полностью – ФИО)

Используются в данной редакции с учебного года 2020/2021

(учебный год цифрами)

Проверено и согласовано «____» _____20___г.

(подпись директора Института/Филиала с расшифровкой)

Москва 2020 г.

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МИРЭА – Российский технологический университет»

МИРЭА

Кафедра КБ-1 "Защита информации"

ЛЕКЦИЯ № 1

по дисциплине: **Б2.В,ДВ.3.1 «Математические основы криптологии 11504»**

(шифр и наименование учебной дисциплины)

по теме: **Ведение. История криптологии в мире и в России. Криптология.Криптография и криптоанализ.Стеганография. Принцип Керкхоффса. Шифр Цезаря. Основные определения.**

(наименование темы лекции)

№

—

МИРЭА – 2020 г.

Тема лекции: Ведение. История криптологии в мире и в России. Криптология.Криптография и криптоанализ.Стеганография. Принцип Керкхоффса. Шифр Цезаря и квадрат Полибия. Основные определения.

Учебные и воспитательные цели:

1. Сформировать у студентов представление о предмете, изучаемом в рамках курса «Математические основы криптологии».
2. Рассмотреть следующие вопросы Криптология.Криптография и криптоанализ.Стеганография. Принцип Керкхоффса. Основные определения. Моноалфавитные шифры. Шифр Цезаря и квадрат Полибия.
3. Привить чувство ответственности за будущую профессию.

Время: 2 часа (90 мин.).

Литература:

а) Основная:

1. Рябко Б.Я.,Фионов А.Н. Криптография в современном мире.-М.: Горячая линия-Телеком, 2018.-300с.:ил.
2. Горбенко А.О., Основы информационной безопасности: введение в профессию.Учебное пособие, СПб: ИЦ «Интермедия», 2016.– 224 с.
3. Бутакова Н.Г., Федоров Н.В. Криптографические методы защиты информации. Учебное пособие, СПб: ИЦ «Интермедия», 2016. – 312 с.
4. Хорев А.А., Защита информации от утечки по техническим каналам. Учебник. СПб: ИЦ «Интермедия», 2016. 920 с.

б) Дополнительная литература:

1. Зайцев А.П. и др. Технические средства и методы защиты информации. Уч. пособие. М.: Горячая линия – Телеком. 2009. – 615 с.
2. Романец Ю.В. и др. Защита информации в компьютерных системах и сетях. М.: Радио и

связь. 1999. – 376 с.
3. Лозовецкий В.В. Информационная безопасность. М.: Изд. ИУИ. 2011. – 169 с.

Учебно-материальное обеспечение:
Наглядные пособия.
Технические средства обучения: проектор.
Приложения: рисунки, таблицы, слайды.

ПЛАН ЛЕКЦИИ:
Введение – до 5 мин.

Основная часть (учебные вопросы) – до 80 мин.
1-й учебный вопрос: История криптологии в мире и в России. -25мин.
2-й учебный вопрос: Криптология. Криптография и криптоанализ.Стеганография.-20 мин.
3-й учебный вопрос: Структура дисциплины, ее особенности, основные понятия и определения. – 15 мин.

3-й учебный вопрос: Моноалфавитные шифры. Шифр Цезаря . Шифр Вернама -20 мин/

Заключение – до 5 мин.

Введение – до 5 мин.
Методические рекомендации:
- показать актуальность темы;
- довести целевую установку через основные положения лекции;
- охарактеризовать место и значение данной темы в курсе;
- описать обстановку, в которой разрабатывалась теоретическая проблема и шла ее практическая реализация;
- дать обзор важнейших источников, монографий, литературы по теме;
- вскрыть особенности изучения студентами материала по рассматриваемой проблеме.
Основная часть – до 80 мин.
Введение

Человечество живёт в информационную эпоху и должно внимательно сохранять информацию о каждом аспекте нашей жизни. Другими словами, *информация* — собственность, и, подобно любой другой собственности, имеет важное *значение*. И в этом качестве *информация* должна быть защищена от нападений.
Информация должна быть сохранена от неправомочного доступа (*конфиденциальность*), защищена от неправомочного изменения (*целостность*) и доступна только разрешенному объекту, когда это ему необходимо (*доступность*).
Несколько десятилетий назад *информация* собиралась на физических носителях. *Конфиденциальность* этих носителей достигалась строгим ограничением доступа, который предоставлялся только людям, имеющим на это право, и тем из них, кому можно было доверить эту информацию. Также нескольким правомочным субъектам разрешалось изменение содержания этих файлов. Готовность была обеспечена тем, что по меньшей мере одному человеку всегда разрешался *доступ* к этим носителям.
С появлением компьютеров хранение информации стало электронным. *Информация* хранилась уже не в физической неэлектронной

среде — она накапливалась в электронной среде (компьютерах). Однако три *требования безопасности* не изменились. Файлы, записанные в компьютере, требовали конфиденциальности, целостности и доступности. Реализация этих требований возможна различными методами и требует решения сложных задач.

В течение прошлых двух десятилетий *компьютерные сети* произвели революцию в использовании информации. *Информация* теперь распределена. Люди при наличии полномочий могут передавать информацию и искать ее на расстоянии, используя *компьютерные сети*. Но три уже упомянутых требования — конфиденциальности, целостности и доступности — не изменились. Они лишь приобрели некоторые новые аспекты. Теперь недостаточно того, что *информация* должна быть конфиденциальной, когда она сохраняется в компьютере. Должен также существовать способ поддержки конфиденциальности, когда эта *информация* передается от одного компьютера к другому.

В этой лекции мы сначала обсуждаем три главных цели поддержки *безопасности информации*.

Когда будет понятно, какие атаки могут угрожать этим трем целям, тогда можно обсудить службы безопасности, предназначенные для этих целей. Потом определяются *механизмы* обеспечения службы безопасности и методы, которые могут использоваться, чтобы осуществить эти *механизмы*.

Сведения из истории криптологии

Исторически *криптография* развивалась как практическая дисциплина, изучающая и разрабатывающая способы шифрования письменных сообщений. В распоряжении историков имеются данные, что криптографические методы применялись в Древнем Египте, Индии, Месопотамии. Так, например, в записях египетских жрецов есть сведения о системах и способах составления шифрованных посланий.

Древние греки оставили документальные подтверждения о различных применяемых ими шифровальных системах. Греками, а вернее спартанцами, во время многочисленных войн применялось одно из первых шифровальных устройств – Сцитала. Сцитала представляла собой цилиндрический жезл определенного диаметра. На Сциталу виток к витку наматывалась узкая полоска папируса (или кожаного ремня). На намотанной ленте вдоль оси жезла писали *открытое сообщение*. Затем ленту разматывали и переправляли адресату. После снятия папируса с жезла выходило как будто буквы сообщения написаны в беспорядке поперек ленты. Если папирус попадал в руки противника, то секретное сообщение прочитать было невозможно. Для получения исходного текста была необходима Сцитала точно такого же диаметра – на нее наматывалась полученная полоска папируса, строки сообщения совмещались, и в результате можно было прочитать секретное послание. Ключом в данном методе шифрования являлся *диаметр* Сциталы. Интересно, что изобретение дешифровального "устройства" приписывается Аристотелю. Предполагается, что именно он предложил использовать конусообразное "копье", на которое наматывалась перехваченная лента с зашифрованным сообщением. Лента с буквами передвигалась вдоль оси конуса до тех пор, пока не появлялся осмысленный текст.

В Древней Греции использовались и другие шифры. Так, например, там был изобретен *шифр*, который в дальнейшем стал называться "квадратом Полибия". Согласно этому шифру буквы сообщения заменялись числами, представляющими собой *координаты* в квадрате 5x5, в который вписаны символы алфавита. Многочисленные исторические документы подтверждают, что в политике и в военном деле широко применялись различные шифры. Диск и линейка ЭНЕЯ. Книжный шифр ЭНЕЯ.

В арабских странах *шифрование* сообщений довольно широко использовалось как в военных, так и в политических целях и даже в переписке между торговыми партнерами. Кстати, *слово* "*шифр*" арабского происхождения, так же как и *слово* "цифра". В VIII – XV веках на свет появляются научные труды, содержащие сведения *по* криптографии: описания различных шифров и даже некоторых методов криптоанализа. Так, в многотомной энциклопедии "Шауба аль-Аша" упоминается о частотном криптоанализе

(то есть анализе, основанном на частоте встречаемости букв открытого и зашифрованного сообщений). В этой же энциклопедии приводится *таблица* частотных характеристик букв арабского языка.

В средние века криптографические методы использовались, прежде всего, в военном деле, шпионаже, дипломатии. Изучением шифров занимались священники, ученые и дипломаты. На практике применялись различные шифры. Первые труды *по* криптографии созданы в XIV – XVI веках Чикко Симоннети (сотрудником папской канцелярии), Габлиэлем де Лавиндой (секретарем папы Клементия XII), Леоном Баттистой Альберти (знаменитым итальянским архитектором и философом), аббатом Иоганнесом Тритемием, жившем в Германии. Все указанные деятели внесли большой вклад в развитие криптографии, так как не только рассматривали в своих трудах существующие шифры, но и предлагали различные усовершенствованные методы шифрования, а также некоторые простейшие методы криптоанализа. Так, например, в трудах Симоннети и де Лавинды предлагаются шифры пропорциональной замены, в которых наиболее часто встречаемым буквам ставится в соответствие несколько символов для выравнивания частоты встречаемости знаков в шифротексте. Леон Альберти, вероятно, первым предложил так называемые полиалфавитные шифры. Нововведение Альберти состояло в том, чтобы использовать несколько замен в соответствии с ключом. Предполагается, что он также изобрёл первую автоматическую шифровальную машину — шифровальный *диск*, который осуществлял частичную реализацию его изобретения.

В XVII-XVIII веках во многих государствах Европы появились специальные шифровальные службы. В России датой появления криптографической службы специалисты называют 1549 год, когда был создан "посольский приказ", в котором имелось "цифирное" отделение. В эпоху Петра I криптографическая служба была реорганизована в "Посольскую канцелярию".

В различные времена криптографией занимались многие политики и ученые. Среди них Пифагор, Аристотель, Платон, Галилей, Д. Порта, Д. Кардано, Л. да Винчи, Ф. Виет, Д. Валлис, Б. *Паскаль*, И. Ньютон, Ф. Бекон, Х. Гольбах, Ф. Эпинус, Л. Эйлер, П.Ф. Шиллинг, Ч. Беббидж и другие.

Огромное влияние на развитие криптографии оказывают достижения научно-технического прогресса. Так, например, в середине XIX века после изобретения телеграфа появилось несколько дипломатических и коммерческих шифров, ориентированных на применение телеграфа. Возрастание скорости передачи данных требовало увеличения скорости шифрования. В конце XIX века появились механические *шифраторы* Т. Джефферсона и Ч. Уитстона. С конца XIX века *криптография* стала серьезной отраслью научных знаний и стала изучаться как отдельная наука в военных академиях.

В XX веке появились новые возможности *по* передаче информации на большие расстояния с большой скоростью. В связи с применением радиосвязи расширились возможности доступа к шифрованной информации в процессе ее передачи. Научно-технический прогресс преобразил криптографию, которая стала вначале электромеханической, а затем электронной. В XX веке возникает специализация в криптографической деятельности. Появляются специалисты *по* шифрованию, *по* перехвату зашифрованных сообщений, *по* дешифрованию шифров противника.

В 20-х годах XX века для автоматизации процесса шифрования появились многочисленные механические устройства. В частности, широко использовались роторные шифровальные машины, в которых для выполнения операций замены символов применялись механические колеса – роторы. Шифровальные машины преобразовывали *открытый текст* в зашифрованный, состоящий из символов того же алфавита. После преобразования зашифрованная *информация* могла передаваться различными способами, например, *по* радиоканалу. Во всех развитых странах, в том числе и в СССР, создавались высокоскоростные шифрмашины, которые широко применялись во время второй мировой войны и позже.

В середине XX века разработкой криптографических алгоритмов стали заниматься профессиональные математики и специалисты в области информатики. Существенное влияние на развитие криптографии оказала работа американского инженера-*математика* К. Шеннона "Теория связи в секретных системах", в которой были сформулированы и математически доказаны условия "невскрываемости" шифров.

С 50-х годов XX века в криптографии используется электронная вычислительная техника. Начинается создание так называемых блочных шифров, которые позволяют обрабатывать информацию целыми фрагментами или блоками. Первоначально для операций *блочного шифрования* разрабатывали аппаратные устройства с жесткой логикой, однако стремительное развитие возможностей вычислительной техники позволило создать программные аналоги блочных систем шифрования. Криптографические программные и *аппаратные средства* стали использоваться в гражданских целях, например, в коммерческих системах передачи информации.

С развитием информационных технологий *криптография* не только приобрела новые сферы применения, но и претерпела значительные изменения. В древние времена в процессе обмена зашифрованными сообщениями участвовало только две стороны, поэтому ключом шифрования необходимо было обеспечить только эти две

стороны. В современных информационных системах в процессе передачи информации задействовано множество абонентов, и все они заинтересованы в надежных и удобных каналах получения ключей шифрования. Проблема *распределения ключей* была решена в двадцатом веке благодаря изобретению нового принципа шифрования – *асимметричного шифрования* или шифрования с открытым ключом (70-е годы XX в.). Основоположниками этого метода шифрования считаются У. Диффи и М. Хеллман. В *асимметричных алгоритмах* шифрования используются специальные математические функции – *односторонние функции*. Открытие асимметричных криптосистем позволило еще больше расширить сферы применения криптографии. Именно *шифрование* с открытым ключом лежит в основе процедур формирования цифровой подписи и проверки подлинности, а следовательно, и в основе принципов работы банковских пластиковых карт, "электронных" денег и других современных технологий.

Новые сферы применения криптографии привлекают математиков к решению криптографических проблем, а также к созданию новых направлений в математике, теории информации и других смежных науках.

Одним из первых, кто создал профессиональную службу по шифровке и дешифровке сообщений, был кардинал Ришелье. В 1628 году в почтамте Парижа был открыт «Черный кабинет». Его возглавил **Антуан Россиньоль, который являлся автором шифра, используемого в будущем вплоть до наполеоновских войн. Ему принадлежит авторство доктрины: «Стойкость военного шифра должна обеспечить секретность за время, необходимое для выполнения приказа. Стойкость дипломатического шифра должна обеспечивать секретность в течение десятилетий».**

Криптография (от греческого тайнопись) – это совокупность идей и методов, связанных с преобразованием информации с целью ее защиты от непредусмотренных пользователей. Информация считается представленной в виде некоторого текста (сообщения). Это – открытый текст. Способ его преобразования в защищенную форму называется шифром, процесс применения шифра – шифрованием, полученный в результате шифрования измененный текст – криптограммой. Перевод криптограммы в исходный открытый текст производится в ходе дешифрования. Взаимно обратные действия шифрования и дешифрования осуществляются с помощью некоторой дополнительной информации, называемой ключом. Именно в ключе спрятан секрет шифра. Без знания ключа чтение криптограммы должно быть значительно затруднено или практически невозможно в пределах разумного интервала времени. Одним из самых давних и до сих пор широко используемых методов криптографической защиты информации является применение так называемых кодовых книг. Кодовая книга – это своего рода словарь, в котором содержится список часто применяемых в секретной переписке слов, целых фраз, цифровых групп и т.п. с указанием для каждого фрагмента того набора символов, которым он будет заменен при шифровании. Кодовая книга и является ключом шифра. Чтобы читать зашифрованные сообщения, их получатель должен знать соответствующие секретные ключи. Как правило, источник сообщения заранее передает их по защищенному каналу. Передача ключей и их хранение – самое уязвимое место в практической криптографии. Известны многочисленные случаи похищения, копирования, покупки кодовых книг, использовавшихся в дипломатической переписке, драматические истории,

связанные с обнаружением секретных ключей при обысках у подозреваемых в шпионаже. Криптография является одной из трех составных частей криптологии – науки о передаче информации в виде, защищенном от несанкционированного доступа. Криптография, как было сказано, занимается шифрованием и дешифрованием сообщений с помощью секретных ключей. Другая часть криптологии – криптоанализ – представляет собой теорию и практику извлечения информации из криптограммы без использования ключа. Основной принцип криптоанализа сформулировал один из его основоположников **бельгийский криптолог Огюст Керкхофс (1835-1903) в 1883 году в книге «Военная криптография»: «При оценке надежности шифра следует допустить, что противнику известно о нем все, кроме ключа».** Третья часть криптологии – аутентификация – объединяет в себе совокупность приемов, позволяющих проверять подлинность источника информации и полученных сообщений. В истории криптологии отчетливо выделяются три периода. Первый – интуитивная криптология, представлявшая собой занятие, доступное узкому кругу изобретательных умов. В их число входили, в частности, многие выдающиеся математики своего времени. Второй период открывается публикацией в 1949 году статьи американского инженера и математика Клода Шеннона (1916-2001) «Теория связи в секретных системах». Под влиянием высказанных в ней идей криптология стала в последующие годы фактически разделом прикладной математики. Третий период начинается с появления в 1978 году новой системы шифрования RSA, в которой американские криптографы Ривест, Шамир и Адлмен впервые реализовали на практике идею организации защищенной связи без передачи секретных ключей. Криптология

вплоть до недавнего времени была глубоко засекречена во всех странах, так как сферой ее применений была в основном защита

государственных и военных секретов. Лишь начиная с 1970-х годов, методы и средства криптологии официально стали использоваться для обеспечения информационной безопасности не только государства, но и частных лиц и организаций. Отметим некоторые ключевые даты в развитии отечественной криптологии в XX веке. 5 мая 1921 года была образована криптографическая служба при ВЧК (Всероссийская чрезвычайная комиссия по борьбе с контрреволюцией и саботажем). 5 мая в нашей стране ежегодно отмечается День шифровальщика. 19 октября 1949 года было принято решение Центрального комитета ВКП(б) (Всесоюзная коммунистическая партия (большевиков)) о создании Главного управления специальной службы (ГУСС) – координатора единой криптографической службы СССР. 19 октября в нашей стране ежегодно отмечается День криптографа. (Заметим для полноты, что криптографическая служба США - Агентство Национальной безопасности – существует с 1952 года). Месяцем ранее, 23 сентября 1949 года, был осуществлен первый набор студентов на закрытое отделение механико-математического факультета МГУ для подготовки кадров в области криптографии. Оно просуществовало до 1957 года. Тогда же, в 1949 году, открылась Высшая школа криптографов (ВШК) с двухлетним обучением, обеспечивавшая получение второго высшего специального образования. В 1960 году ВШК была преобразована в технический факультет Высшей школы КГБ (Комитет государственной безопасности). В 1992 году был создан Институт криптографии, связи и информатики (ИКСИ) в составе Академии ФСБ России. В Доктрине информационной безопасности Российской Федерации, принятой в 2000 году, отмечается, что «подготовка специалистов с высшим

образованием в области информационной безопасности относится к важнейшим организационно-техническим методам обеспечения информационной безопасности РФ». С середины 1990-х годов в ряде вузов страны начала развертываться система подготовки кадров в естественнонаучном и техническом направлениях в области информационной безопасности, в том числе и по разделам криптологии.

Криптология. Криптография и криптоанализ. Стеганография.

Проблемой защиты информации при ее передаче между абонентами люди занимаются на протяжении всей своей истории. Человечеством изобретено множество способов, позволяющих в той или иной мере скрыть смысл передаваемых сообщений от противника. На практике выработалось несколько групп методов защиты секретных посланий. Назовем некоторые из них, применяющиеся так же давно, как и криптографические.

Первым способом является *физическая защита* материального носителя информации от противника. В качестве носителя данных может выступать бумага, компьютерный носитель (DVD-*диск*, флэш-карта, магнитный *диск*, *жесткий диск* компьютера и т.д.). Для реализации этого способа необходим надежный *канал связи*, недоступный для перехвата. В различное время для этого использовались почтовые голуби, специальные курьеры, радиопередачи на секретной частоте. Методы физической защиты информации используются и в современных автоматизированных системах обработки данных. Так, например, комплексные системы защиты информации невозможны без систем ограждения и физической изоляции, а также без охранных систем.

Второй способ защиты информации, известный с давних времен – *стеганографическая защита* информации. Этот способ защиты основан на попытке скрыть от противника сам факт наличия интересующей его информации. При стеганографическом методе защиты от противника прячут физический носитель данных или маскируют секретные сообщения среди открытой, несекретной информации. К таким способам относят, например, "запрятывание" микрофотографии с тайной информацией в несекретном месте: под маркой на почтовом конверте, под обложкой книги и т.д. К стеганографии относятся также такие известные приемы, как "запрятывание" секретного послания в корешках книг, в пуговицах, в каблуках, в пломбе зуба и т.д. Некоторые из методов были разработаны еще в древние времена. Так, например, греки нашли необычное решение: они брили наголо голову раба и выцарапывали на ней свое послание. Когда волосы на голове раба отрастали вновь, его посылали доставить сообщение. Получатель брил голову раба и прочитывал текст. К сожалению, на отправку сообщения и получение ответа таким способом уходило несколько недель.

В более поздние времена в этом направлении наибольшее распространение получили химические (симпатические) чернила. Текст, написанный этими чернилами между строк несекретного сообщения, невидим. Он появлялся только в результате применения определенной технологии проявления.

В условиях повсеместного использования информационных технологий возникают новые стеганографические приемы. Например, известен способ, при котором секретное сообщение прячется в файле графического изображения. При использовании этого способа младший значащий *бит* в описании каждого пикселя изображения заменяется битом сообщения. Разделив все исходное сообщение на биты и разместив эти

биты *по* всему графическому файлу, мы пересылаем изображение с замаскированным сообщением получателю. Графическое изображение при этом меняется не слишком сильно, особенно если использовался режим с большим количеством цветов, например, с глубиной цвета 24 бита на *пиксел*. Это связано с тем, что человеческий глаз не может различать такое большое количество цветов. В результате в картинке размером всего 32 на 32 точки можно вместить тайное сообщение длиной 1024 бита или 128 *байт*.

Третий способ защиты информации – наиболее надежный и распространенный в наши дни – *криптографический* . Этот метод защиты информации предполагает преобразование информации для сокрытия ее смысла от противника. **Криптография** в переводе с греческого означает "тайнопись". В настоящее время *криптография* занимается поиском и исследованием математических методов преобразования информации.

Наряду с криптографией развивается и совершенствуется **криптоанализ** – наука о преодолении криптографической защиты информации. Криптоаналитики исследуют возможности расшифровывания информации без знания ключей. Успешно проведенный *криптоанализ* позволяет получить *ключ шифрования*, или *открытый текст*, или то и другое вместе. Иногда криптографию и *криптоанализ* объединяют в одну науку – **криптологию** (kryptos - тайный, logos - наука), занимающуюся вопросами обратимого преобразования информации с целью защиты от несанкционированного доступа, оценкой надежности систем шифрования и анализом стойкости шифров.

В настоящее время *криптография* прочно вошла в нашу жизнь. Перечислим лишь некоторые сферы применения криптографии в современном информатизированном обществе:

- шифрование данных при передаче по открытым каналам связи (например, при совершении покупки в Интернете сведения о сделке, такие как адрес, телефон, номер кредитной карты, обычно зашифровываются в целях безопасности);
- обслуживание банковских пластиковых карт;
- хранение и обработка паролей пользователей в сети;
- сдача бухгалтерских и иных отчетов через удаленные каналы связи;
- банковское обслуживание предприятий через локальную или глобальную сеть;
- безопасное от несанкционированного доступа хранение данных на жестком диске компьютера (в операционной системе Windows даже имеется специальный термин – шифрованная файловая система (EFS)).

До начала XX века криптографические методы применялись лишь для шифрования данных с целью защиты от несанкционированного доступа. В двадцатом веке в связи с развитием техники передачи информации на дальние расстояния интерес к криптографии значительно возрос. Благодаря созданию новых криптографических методов расширился и спектр задач криптографии. В настоящее время считается, что *криптография* предназначена решать следующие задачи:

- собственно шифрование данных с целью защиты от несанкционированного доступа;
- проверка подлинности сообщений: получатель сообщения может проверить его источник;
- проверка целостности передаваемых данных: получатель может проверить, не было ли сообщение изменено или подменено в процессе пересылки;
- обеспечение невозможности отказа, то есть невозможности как для получателя, так и для отправителя отказаться от факта передачи.

Системы шифрования варьируются от самых элементарных до очень сложных. И если первые не требуют никаких математических познаний, то в последних используются понятия, знакомые лишь специалистам в некоторых областях математики и информатики. При использовании криптографических методов должны учитываться *затраты* на защиту информации и на реализацию методов нападения. На практике стремятся к достижению компромисса между стоимостью шифрования и требуемой степенью обеспечения безопасности.

В рамках данного учебного пособия рассматриваются как простейшие, "докомпьютерные", шифры, известные человечеству на протяжении веков, так и современные системы шифрования, разработанные только в XXI веке.

Моноалфавитные шифры. Шифр Цезаря.(12.07.100- 15.03.44)

Шифр Цезаря(veni, vidi, vici)

Теперь, когда даны основные определения, рассмотрим одну из простейших систем шифрования, которая носит имя "*шифр* Юлия Цезаря". Предполагается, что знаменитый римский император и полководец, живший в 1 веке до нашей эры, использовал этот *шифр* в своей переписке.

Шифр Цезаря применительно к русскому языку пример 1.1 состоит в следующем. Каждая буква сообщения заменяется на другую, которая в русском алфавите отстоит от исходной на три позиции дальше. Таким образом, буква А заменяется на Г , Б на Д и так далее вплоть до буквы Ь , которая заменялась на Я , затем Э на А , Ю на Б и, наконец, Я на В .

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ

Так, например, *слово* **ЗАМЕНА** после шифрования методом Цезаря превратится в **КГПЗРГ** .

Это не очень сложный метод, тем более что при шифровании сообщений из нескольких слов сразу становится понятным, сколько слов содержал исходный текст. Кроме того, можно получить некоторую информацию *по* анализу повторов букв в зашифрованном сообщении. Например, в зашифрованном **КГПЗРГ** одна из букв повторяется дважды. Тем не менее, Цезарь вошел в историю криптографии, а "*шифр* Юлия Цезаря", как его до сих пор называют, служит примером одной из первых систем шифрования.

Для расшифрования сообщения **КГПЗРГ** необходимо знать только сам *алгоритм* шифрования. Любой человек, знающий способ шифрования, легко может расшифровать секретное сообщение. Таким образом, ключом в данном методе является сам *алгоритм*.

Каким образом можно усовершенствовать *шифр* Цезаря? Можно было бы попытаться расширить *алфавит* с 33 до 36 символов и более за счет включения знаков препинания и пробелов. Это увеличение алфавита замаскировало бы длину каждого отдельного слова.

В криптографии принято считать, что противник может знать использованный *алгоритм* шифрования, характер передаваемых сообщений и перехваченный шифротекст, но не знает *секретный ключ*. Как уже упоминалось выше, это называется принципом Керкхоффса. Иногда это правило кажется "перестраховкой", но такая "перестраховка" отнюдь не лишняя, если, например, передаются данные оборонного или государственного характера.

Усовершенствуем *шифр* Цезаря с учетом правила Керкхоффса.

Однако еще в XIX веке специалисты в области криптографии предположили, что секретность алгоритма шифрования не является гарантией от взлома. Более того, в дальнейшем было понято, что *по*-настоящему надежная система шифрования должна оставаться защищённой, даже если противник полностью узнал *алгоритм* шифрования. Секретность ключа должна быть достаточна для хорошего шифра, чтобы сохранить стойкость к попыткам взлома. Этот фундаментальный принцип впервые был сформулирован в 1883 Керкхоффсом (A. Kerckhoffs) и обычно называется **принципом Керкхоффса**.

Предположим, что буквы сдвигаются не на три знака вправо, а на **n (0<n<33)**. В этом случае в системе шифрования появляется *ключ* – число **n** – *параметр* сдвига. Отправитель и получатель могут каким-либо образом договариваться (например, лично) и иногда менять *значение* ключа. Так как n может принимать разные значения, *знание* одного только алгоритма не позволит противнику расшифровать секретное сообщение.

Каким же образом может действовать в том случае *злоумышленник*, чтобы узнать содержание сообщения? Пусть, например, перехвачено секретное сообщение **ЧСЮЭЮЪ**. Противнику известно, что *ключ* (*параметр* сдвига n) может принимать значения от 1 до 32. Пытаясь найти *значение* секретного ключа, мы будем проводить атаку *по* шифротексту. Рассмотрим способ последовательного перебора всех возможных ключей (это так называемый метод "грубой силы"). Запишем на 32 строчках все варианты, которые получаются сдвигом каждой буквы на 1, 2, 3, ... , 32 позиции соответственно. Эту операцию можно проводить вручную, а можно составить несложную программу, которая запишет все варианты перебора параметра n в *файл*. Одна из этих 32 строк будет содержать исходное сообщение (таблица 1.1).

Таблица 1.1. Перебор вариантов для поиска ключа при использовании метода Цезаря

Перехваченная криптограмма **ЧСЮЭЮЪ**		
1	**ШТЯЮЯЫ**	**17**
2	**ЩУАЯАЬ**	**18**
3	**ЪФБАБЭ**	**19**
4	**ЫХВБВЮ**	**20**

5	**ЬЦГВГЯ**	**21**
6	**ЭЧДГДА**	**22**
7	**ЮШЕДЕБ**	**23**
8	**ЯЩЁЕЁВ**	**24**
9	**АЪЖЁЖГ**	**25**
10	**БЫЗЖЗД**	**26**
11	**ВЬИЗИЕ**	**27**
12	**ГЭЙИЙЁ**	**28**
13	**ДЮКЙКЖ**	**29**
14	**ЕЯЛКЛЗ**	**30**
15	**ЁАМЛМИ**	**31**
16	**ЖБНМНЙ**	**32**

Мы видим, что единственное *слово*, имеющее смысл, – это **ЗВОНОК**. Это *слово* располагается на 17 месте. Следовательно, если шифрованный текст сдвинуть на 17 позиций вперед получится *открытый текст*. Это означает, что для получения шифрованного текста *открытый текст* нужно сдвинуть на `(33-17)=16` позиций. Таким образом, получили, что при шифровании *ключ* `n=16`.

Так как ни при каком другом сдвиге не получилось осмысленного сообщения, то, скорее всего, мы правильно дешифровали это сообщение. Такое допущение о единственности решения вполне обоснованно, когда исходное сообщение составлено на одном из естественных языков (в рассмотренном примере – русском) и содержит более пяти-шести знаков. Но если сообщение очень короткое, возможных решений может быть несколько. Единственное решение также очень трудно найти, если исходное сообщение, состоит, например, из цифр.

Так, например, пусть исходный *алфавит* состоит из арабских цифр, то есть имеет вид

0 1 2 3 4 5 6 7 8 9.

Один из абонентов желает переслать другому секретный код замка, состоящий из пяти цифр и равный `12345`. Отправитель и получатель заранее договорились о том, что *ключ шифрования* `n` будет равен `3`. Отправитель шифрует выбранным ключом исходное сообщение `12345`, получает `45678` и переправляет полученное *значение* своему абоненту. Возможно, противник перехватит криптограмму и попытается вскрыть ее, используя, как и раньше, метод последовательного перебора. Так как исходный *алфавит* состоял из `10` символов, то *значение* ключа может лежать в диапазоне от `1` до `9`. Выпишем, как и раньше все варианты, которые получаются сдвигом каждого знака перехваченного сообщения на `1, 2, 3, ... , 9` позиций соответственно (таблица 1.2).

Таблица 1.2. Перебор вариантов для вскрытия зашифрованного кода замка

Перехваченная криптограмма **45678**	
1	56789
2	67890
3	78901
4	89012
5	90123
6	01234
7	12345
8	23456
9	34567

Видно, что все полученные варианты равнозначны и *злоумышленник* не может понять, какая именно комбинация истинна. Анализируя шифротекст, он не может найти значения секретного ключа. Конечно, один из приведенных в таблице вариантов подойдет к кодовому замку, но в столь простом методе шифрования нельзя рассчитывать на большую секретность.

В первом примере сообщение — текст на русском языке, поэтому оно подчиняется многочисленным правилам, различные буквы и их *сочетания* имеют различные вероятности и, в частности, многие наборы букв вообще запрещены. (Это свойство называется избыточностью текста). Поэтому-то и удалось легко подобрать *ключ* и дешифровать сообщение, т.е. *избыточность* позволила "взломать" *шифр*. В противоположность этому, во втором примере все комбинации цифр допустимы. "Язык" кодового замка не содержит избыточности. Поэтому даже простой *шифр*, примененный к сообщениям этого языка, становится невскрываемым в случае атаки

только *по* шифротексту. Если же мы имеем возможность проводить атаку и *по* открытому тексту, то есть имеем пары "*открытое сообщение*" – "зашифрованное сообщение", то раскрытие становится совершенно простым как в случае использования символов-букв, так и в случае символов-цифр.

Приведенные простые примеры показывают, что *вероятность* успешного криптоанализа зависит от многих факторов: от системы шифрования, от длины перехваченного сообщения, от *языка и алфавита* исходного сообщения. В последующих лекциях постараемся подробнее рассмотреть все эти факторы.

Одноразовый шифровальный блокнот (шифр Вернама). В шифре «одноразовый блокнот», как и в шифре Виженера, преобразование текста производится с использованием ключа в соответствии с формулами (1.3), (1.4). Однако к ключевой последовательности предъявляются определенные требования, позволяющие сделать этот шифр безусловно стойким:

- • выбор ключа из ключевого пространства должен осуществляться равновероятно (ключ является абсолютно случайной последовательностью);
- • длина ключа должна быть не короче длины открытого сообщения;
- • ключ должен использоваться только один раз.

В случае применения системы одноразового шифровального блокнота используется ключ потенциально бесконечной длины с неограниченным количеством возможных комбинаций.

Шифр был предложен в конце Первой мировой войны американским инженером Г. Бернамом (Gilbert Vernam). Первым этапом, по замыслу разработчиков этого шифра, является подготовка блокнота, состоящего из сотен бумажных листов. На каждом листе находится уникальный ключ в виде длинной абсолютно случайной последовательности букв. Предполагается, что длина таких последовательностей достаточна для шифрования, т.е. возможные шифруемые сообщения будут заведомо короче. Подготавливаются два варианта блокнота: один — для отправителя, другой — для получателя.

Чтобы зашифровать сообщение, отправитель пользуется шифром Вернама, применяя ключ, напечатанный на первом листе блокнота. Получатель сможет легко расшифровать сообщение шифром Вернама, пользуясь идентичным ключом (с того же листа копии блокнота).

После того, как сообщение было успешно отправлено, получено и расшифровано, оба — и отправитель, и получатель — уничтожают лист с использованным ключом, чтобы никогда уже больше им не пользоваться.

При шифровании следующего сообщения будет использован следующий случайный ключ из блокнота, который затем также будет уничтожен, и т.д. Поскольку каждый лист используется только один раз, эта система шифрования получила название «одноразовый шифровальный блокнот» (one time pad).

Методика шифрования с использованием одноразового шифровального блокнота обладает исключительной надежностью. Поскольку ключ абсолютно случаен, не представляется возможным восстановить его на основании анализа языковых

конструкций. Перебор всех возможных вариантов ключей, даже если не учитывать трудоемкость этого процесса, также не приведет к успеху. Результатом такого перебора станут все возможные осмысленные сообщения данной длины, при этом невозможно определить, какое из них окажется истинным, а какие — ложными.

Пусть нормативный алфавит состоит из 32 символов русского языка (буквы

«е» и «ё» не различаются) и пробела, использован шифр Вернама. Тогда при дешифровании криптограммы «ржъхадсюдай» ключом «квтцр орафл» будет получен текст «жди сегодня», а ключом «нфцвбюсьусй» — текст «буду завтра».

Поскольку ключ абсолютно случаен, то варианты ключа «квтцр орафл» и «пфцвбюсьусй» равноценны и невозможно отдать предпочтение какому-то одному из них. Поэтому невозможно определить, какой из этих двух (и других правдоподобных) вариантов открытого текста является истинным.

Узнать, является ли полученный результат дешифрования в действительности оригинальным сообщением, противник сможет, лишь получив в свое распоряжение копию шифровального блокнота.

Стойкость системы одноразового шифровального блокнота обусловлена случайным характером ключа. Невозможность вскрытия такого шифра можно доказать математически. В то же время шифр Вернама достаточно чувствителен к любым нарушением методики шифрования, например к повторному использованию ключа или его неслучайности.

При всей привлекательности, для этого метода шифрования существуют определенные ограничения, которые затрудняют его использование на практике, в том числе и в компьютерных системах (например, для защищенной передачи информации в компьютерной сети).

Проблема создания случайных ключей. На практике затруднительно создавать большое количество абсолютно случайных ключевых последовательностей. Например, реализовать программно выбор истинно случайной последовательности чисел невозможно. Так называемые программные «генераторы случайных чисел» генерируют не истинно случайные, а псевдослучайные последовательности. При этом используются функции

специального вида, т.е. достаточно сложные, но вполне определенные закономерности, значения которых имеют статистическое распределение, близкое к распределению случайных чисел. Конкретный вид последовательности псевдослучайных чисел обычно задается некоторыми начальными параметрами функции-генератора.

Другим требованием, которое невозможно реализовать программно, является потенциальная бесконечность ключа. Поскольку ключ в системе одноразового шифровального блокнота должен быть не короче любого сообщения, которое потребуется зашифровать, то в общем случае он потенциально бесконечен. Реализуемые программно генераторы псевдослучайных чисел — периодические функции, значения которых циклически повторяются. Длина периодически повторяющегося фрагмента псевдослучайной последовательности (в рамках которого нет повторений) называется периодом функции-генератора. Период — всегда конечное, хотя, возможно, и достаточно большое число.

В настоящее время существуют аппаратные реализации генераторов истинно случайных чисел. Такие устройства работают, получая числа на основе различного вида непредсказуемых входных данных, например измеряя значения случайных физических величин (параметры радиоактивного распада, колебания атмосферных условий, незначительные изменения электрического тока). Поскольку входные данные всегда меняются, невозможно получить две одинаковые последовательности случайных чисел, т.е. числа являются неповторяющимися.

Тем не менее при практическом использовании одноразового шифровального блокнота существуют и другие сложности.

Проблема распределения ключей. Для того чтобы восстановить открытый текст, надо воспользоваться тем же ключом, поэтому возникает проблема передачи копии блокнота получателю. Если связь осуществляется между несколькими абонентами, идентичные копии шифровальных блокнотов необходимо передать всем одновременно. Более того, если злоумышленник перехватит хотя бы один комплект ключей, то надежность всей коммуникационной системы будет нарушена.

Проблема синхронизации ключей. При организации защищенной связи между несколькими абонентами каждый из них должен быть уверен в том, что он использует нужный лист блокнота в нужное время. Если кто-то уже использовал данный лист, то повторное использование может привести ко взлому шифра. Существует также проблема

синхронизации последовательности ключей у отправителя и получателя сообщения, например недоставка сообщения влечет рассинхронизацию использования ключей.

Основные определения

Теперь, узнав назначение криптографии, познакомимся с основными терминами, которые будем использовать при изучении криптографических методов защиты информации.

Шифр – совокупность заранее оговоренных способов преобразования исходного секретного сообщения с целью его защиты.

Исходные сообщения обычно называют **открытыми текстами**. В иностранной литературе для открытого текста используют термин **plaintext**.

Символ - это любой знак, в том числе буква, цифра или знак препинания.

Алфавит - конечное множество используемых для кодирования информации символов. Например, русский *алфавит* содержит 33 буквы от `А` до `Я` . Однако этих тридцати трех знаков обычно бывает недостаточно для записи сообщений, поэтому их дополняют символом пробела, точкой, запятой и другими знаками. *Алфавит* арабских цифр – это символы `0, 1, 2, 3, 4, 5, 6, 7, 8, 9` . Этот *алфавит* содержит 10 знаков и с его помощью можно записать любое *натуральное число*. Любое сообщение может быть записано также с помощью *двоичного алфавита* , то есть с использованием только нулей и единиц.

Сообщение, полученное после преобразования с использованием любого шифра, называется **шифрованным сообщением** (закрытым текстом, криптограммой). В иностранной литературе для закрытого текста используют термин **ciphertext**.

Преобразование открытого текста в криптограмму называется **зашифрованием**. Обратное действие называется **расшифрованием**. В англоязычной литературе терминам "зашифрование/ *расшифрование*" соответствуют термины **"enciphering/deciphering"**.

Ключ – *информация*, необходимая для шифрования и расшифрования сообщений.

С точки зрения русского языка термины "*расшифрование*" и "*дешифрование*" являются синонимами. Однако в работах *по* криптографии последних десятилетий часто эти слова различают. Будем считать, что термины "*расшифрование*" и "*дешифрование*" не являются синонимами. Примем, что *расшифрованием* занимается легальный *получатель сообщения* (тот, кто знает *ключ*), а человек, которому послание не предназначено, пытаясь понять его смысл, занимается *дешифрованием* .

Система шифрования, или **шифрсистема**, – это любая система, которую можно использовать для обратимого изменения текста сообщения с целью сделать его непонятным для всех, кроме тех, кому оно предназначено.

Криптостойкостью называется характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа (т.е. способность противостоять криптоанализу).

Таким образом, с учетом всех сделанных определений можно дать более точное *определение* науке "*криптография*". **Криптография** изучает построение и использование систем шифрования, в том числе их стойкость, слабости и степень уязвимости относительно различных методов вскрытия.

Все методы преобразования информации с целью защиты от несанкционированного доступа делятся на две большие группы: методы шифрования *с закрытым ключом* и методы шифрования *с открытым ключом* . **Шифрование с закрытым ключом** (*шифрование* с секретным ключом или *симметричное шифрование*) используется человеком уже довольно долгое время. Для шифрования и расшифрования данных в этих методах используется один и тот же *ключ*, который обе стороны стараются хранить в секрете от противника. Системы шифрования с закрытым ключом подробно рассматриваются в лекциях 2-9. **Шифрование с открытым ключом** (*асимметричное шифрование*) стало использоваться для криптографического закрытия информации лишь во второй половине XX века. В эту группу относятся методы шифрования, в которых для шифрования и расшифрования данных используются два разных ключа. При этом один из ключей (открытый *ключ*) может передаваться *по* открытому (незащищенному) каналу связи. Алгоритмам преобразования информации с открытым ключом посвящены лекции 10-14 учебного пособия.

Электронной (цифровой) подписью называется обычно присоединяемый к сообщению *блок данных*, полученный с использованием криптографического преобразования. *Электронная подпись* позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения.

Криптографическая система защиты информации – система защиты информации, в которой используются криптографические методы для шифрования данных.

Дополнение к шифру Цезаря.(Практические занятия- 1,2)

Рассмотрим английский алфавит –первая строка таблицы № 1:

A	B	C	D	E	F	G	H	I	J	K	L	N	M	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	N	M	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Табл. №1.

Если в первой строке сдвинуть все буквы последовательно на 3 позиции влево и записать их во вторую строку, и применяя для написания открытого текста, буквы из второй строки мы получим шифр Цезаря.

Например :

Зашифруем знаменитое изречение Цезаря (на английском языке)

ПРИШЕЛ, УВИДЕЛ, ПОБЕДИЛ.(CAME, SAW,WAN).

CAME---FDQH, SAW---VDZ, WAN---ZAP.

Если присвоить буквам цифровые значения, то Табл. №1 примет вид Табл. №2

A	B	C	D	E
01	02	03	04	05

Табл. №2.

D	E	F	G	H	I	J	K	L	N	M	O	P	Q	R	S	T	U	V	W	X
04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24

Табл. №3

В цифровом виде слова Цезаря -

ПРИШЕЛ, УВИДЕЛ, ПОБЕДИЛ.(CAME, SAW,WAN).

CAME---FDQH --06041708 SAW---VDZ ------220426, WAN---ZAP-
---260416.

ZENITH---0308162311

Квадрат Полибия:

СОСТАВЛЯЕТСЯ ТАБЛИЦА В ПРОИЗВОЛЬНОЙ ФОРМЕ.

НАХОДИТСЯ ЯЧЕЙКА С НУЖНОЙ БУКВОЙ И В ШИФРОВАННЫЙ ТЕКСТ ВСТАВЛЯЕТСЯ БУКВА РАСПОЛОЖЕННАЯ В НИЖНЕЙ ОТ НЕЕ ЯЧЕЙКИ В ТОМ ЖЕ СТОЛБЦЕ.

ЕСЛИ БУКВА БУДЕТ В НИЖНЕЙ ЯЧЕЙКЕ- ЗАПИСЫВАЕТСЯ БУКВА ИЗ ВЕРХНЕЙ ЯЧЕЙКИ ТОГО ЖЕ СТОЛБЦА

Ю	**Ж**	**Х**	**З**	**Д**	**Б**
Л	**Щ**	**Ш**	**О**	**Т**	**И**
Ы	**Г**	**С**	**Н**	**П**	**М**
А	**Е**	**К**	**В**	**Ч**	**Я**
Р	**У**	**Ц**	**Ф**	**Ь**	**Э**

Секретное сообщение – КУЦЮУПВНУ КННИГУВМУ